Examiner-Initiated Interview Summary	**Application No.** 10/043,654	**Applicant(s)** BUNKER V. ET AL.	
	Examiner Tongoc Tran	**Art Unit** 2134	

All Participants: **Status of Application:** _____

(1) Tongoc Tran. (3) _____.

(2) Brian Walker. (4) _____.

Date of Interview: 3 October 2007 **Time:** _____

Type of Interview:
☒ Telephonic
□ Video Conference
□ Personal (Copy given to: □ Applicant □ Applicant's representative)

Exhibit Shown or Demonstrated: □ Yes □ No
If Yes, provide a brief description:

Part I.

Rejection(s) discussed:
U.S.C. 102

Claims discussed:
1

Prior art documents discussed:
Gleichauf et al. (U.S. Patent No. 6,324,656)

Part II.

SUBSTANCE OF INTERVIEW DESCRIBING THE GENERAL NATURE OF WHAT WAS DISCUSSED:
See Continuation Sheet

Part III.

□ It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview directly resulted in the allowance of the application. The examiner will provide a written summary of the substance of the interview in the Notice of Allowability.

□ It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview did not result in resolution of all issues. A brief summary by the examiner appears in Part II above.

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

(Examiner/SPE Signature) (Applicant/Applicant's Representative Signature – if appropriate)

Continuation Sheet (PTOL-413B) **Application No. 10/043,654**

Continuation of Substance of Interview including description of the general nature of what was discussed: Examiner and Applicant's representative discussed claimed limitation and the prior art interpretation. Paragraphs 0017 and 0078 of the Specification have been referencing to during the discussion and Applicant's representative agrees to amend the claims to further distinguish the claimed invention from the cited prior art. .

1. (Currently Amended) A network security testing apparatus comprising:

at least one [[a]] first tester for generating a security vulnerability attack simulation comprised of a plurality of waves of tests for iteratively testing for network security vulnerabilities of a network system under test~~-that-~~, the at least one first tester is adapted to communicably couple to [[a]] the network system under test, said at least one first tester adapted to ~~sequentially~~ iteratively perform a plurality of waves of ~~a plurality of sequential~~ tests on the system under test to obtain network security vulnerability information;

wherein each [[of]] test in the plurality of ~~sequential~~ waves of tests are adapted to return the network security vulnerability information regarding the network system under test, the network security vulnerability information provided by each [[of]] test in the plurality of ~~sequential~~ waves of tests being more specific to the network system under test than the network security vulnerability information provided by a previous test;

wherein each [[of]] test in the plurality of ~~sequential~~ waves of tests are ~~more~~ specifically ~~configured~~-modified in real-time to adapt to [[the]]discovered security obstacles of the network system under test detected based on the network security vulnerability information gained from the previous test and to obtain additional network security vulnerability information from the network system under test.

2. (Currently Amended) The network security testing apparatus of claim 1, wherein each of the plurality of ~~sequential~~ iterative tests are more specifically configured to adapt to system configuration of the network system under test based on the network security vulnerability information gained from the previous test and obtain the additional network security vulnerability information from the network system under test.

3. (Canceled)

4. (Currently Amended) The network security testing apparatus of claim [[3]] 1, wherein the network security vulnerability information includes information regarding network connectivity from the at least one first tester to the network system under test.

5. (Canceled)

6. (Previously Presented) The network security testing apparatus of claim1, wherein the network security vulnerability information includes connection information relating to an IP address used in the previous test.

7. (Currently Amended) The network security testing apparatus of claim [[3]] 1, further comprising:

[[a]] at least one second tester that is adapted to communicably couple to the network system under test;

wherein the previous test is executed by said at least one first tester;

wherein determination of whether a subsequent test is executed by said at least one first tester or by said at least one second tester is made based at least partially upon the network security vulnerability information obtained by the previous test in order to adapt to the discovered security obstacles of the network under test.

8. (Previously Presented) The network security testing apparatus of claim 7, wherein the subsequent test includes execution of a test tool selected from a plurality of test tools based at least partially upon the network security vulnerability information obtained by the previous test.

9. (Canceled)

10. (Previously Presented) The network security testing apparatus of Claim 1, wherein the plurality of tests continue until all relevant information about the system under test has been collected.

11. (Previously Presented) The network security testing apparatus of claim 7, wherein the subsequent test includes execution of a test tool selected from a plurality of test tools based at least partially upon the system environment information.

12. (Canceled)

13. (Currently Amended) A network security testing method comprising:

a) executing a first [[test]] wave of tests in a security vulnerability attack simulation by [[a]] at least one first tester to test for network security vulnerabilities of a network system under test, wherein the first [[test]] wave of tests is targeted at [[a]] the network system under test, and wherein the at least one first tester is communicably coupled to the network system under test;

b) receiving first information from the first [[test]] wave of tests about the network system under test, after executing the first [[test]] wave of tests, the first information comprising network security vulnerability information;

c) executing a second [[test]] wave of tests in a security vulnerability attack simulation to test for the network vulnerabilities of the network system under test after said receiving first information, wherein the second [[test]] wave of tests is [[more]] specifically ~~configured~~ modified in real time to adapt to [[the]] discovered security obstacles of the network system under test detected based on the network security vulnerability information gained from the first [[test]] wave of tests and obtain ~~second~~ additional network security vulnerability information from the network system under test based on the first information, the ~~second~~ additional network security vulnerability information ~~comprising additional network security vulnerability information~~ is more specific to the network system under test than the first information;

d) receiving the ~~second~~ additional network security vulnerability information from the second [[test]] wave of tests about the network system under test, after executing the second [[test]] wave of tests;

e) repeating steps a)-d) a plurality of times until relevant information about the system under test has been collected; and

f) wherein the network security vulnerability information obtained from each subsequent [[test]] wave of tests is more specific to the system under test based on the network security vulnerability information provided by each previous test.

14. (Currently Amended) The network security testing method of claim 13, wherein the time period between said executing the first [[test]] wave of tests and said executing the second [[test]] wave of tests can be negligible.

15. (Canceled)

16. (Previously Presented) The network security testing method of claim 13, wherein said network security vulnerability information comprises information regarding network connectivity from the first tester to the network system under test.

17. (Canceled)

18 (Previously Presented) The network security testing method of claim 13, wherein said receiving network security vulnerability information comprises receiving connection information relating to an IP address used in said executing the first test.

19. (Currently Amended) The network security testing method of claim 13, further comprising determining whether ~~the second test~~ a test in the second wave of tests will be executed by the at least one first tester or by [[a]] at least one second tester based upon the network security vulnerability information from the first test, before said executing the second test.

20. (Currently Amended) The network security testing method of claim 13, further comprising selecting the ~~second~~ test in the second wave of tests from a plurality of tests based at least partially upon the network security vulnerability information.

21. (Previously Presented) The network security testing method of claim 13, further comprising:

determining whether all possible network security vulnerability information regarding the system under test has been received in light of the plurality of tests; and executing additional tests until all possible network security vulnerability information regarding the system under test has been received in light of the plurality of tests.

22. (Canceled)

23. (Currently Amended) The network security testing method of claim 19, further comprising selecting the ~~second~~ test in the second wave of tests from a plurality of tests based at least partially upon the network security vulnerability information.

24. (Canceled)

25. (Currently Amended) A computer program product for network security testing stored in a computer-readable medium, comprising:

a) instructions for executing a first [[test]] wave of tests in a security vulnerability attack simulation by [[a]] at least one first tester to test for network security vulnerabilities of a network system under test, wherein the first [[test]] wave of tests is targeted at [[a]] the network system under test, and wherein the at least one first tester is communicably coupled to the network system under test;

b) instructions for receiving first information from the first [[test]] wave of tests about the network system under test, after executing the first [[test]] wave of tests, the first information comprising network security vulnerability information;

c) instructions for executing a second [[test]] wave of tests to test for the network security vulnerabilities of the network system under test after said receiving first information, wherein the second [[test]] wave of tests is ~~more~~ specifically ~~configured~~ modified in real time to adapt to the discovered security obstacles of the network system under test detected based on the network security vulnerability information gained from the first [[test]] wave of tests and obtain ~~second~~ additional network security vulnerability information from to the network system under test based on the first information, the ~~second~~ additional network security vulnerability information ~~comprising additional network security vulnerability information~~ is more specific to the network system under test than the first information;

d) instructions for receiving the ~~second~~ additional network security vulnerability information from the second [[test]] wave of tests about the network system under test, after executing the second [[test]] wave of tests;

e) instructions for repeating steps a)-d) a plurality of times until all relevant information about the system under test has been collected; and

f) instructions for wherein the network security vulnerability information obtained from each subsequent [[test]] wave of tests is more specific to the system under test based on the network security vulnerability information provided by each previous test.

26. (Currently Amended) The computer program product of claim 25, wherein the time period between executing the first [[test]] wave of tests and executing the second [[test]] wave of tests can be negligible.

27. (Canceled)

28. (Currently Amended) The computer program product of claim 25, wherein said network security vulnerability information comprises information regarding network connectivity from the at least one first tester to the network system under test.

29. (Canceled)

30. (Currently Amended) The computer program product of claim 25, wherein receiving network security vulnerability information comprises receiving session establishability information relating to an IP address used in executing the first test.

31. (Previously Presented) The computer program product of claim 25, further comprising instructions for determining whether ~~the second test~~ a test in the second wave of tests will be executed by the at least one first tester or by [[a]] at least one second tester based upon the network security vulnerability information from the first test, before said executing the second test.

32. (Previously Presented) The computer program product of claim 25, further comprising instructions for selecting the ~~second~~ test in the second wave of tests from a plurality of tests based at least partially upon the network security vulnerability information.

33. (Previously Presented) The computer program product of claim 25, further comprising:

instructions for determining whether all possible network security vulnerability information regarding the system under test has been received in light of the plurality of tests; and

instructions for executing additional tests until all possible network security vulnerability information regarding the system under test has been received in light of the plurality of tests.

34. (Canceled)

35. (Currently Amended) The computer program product of claim 31, further comprising instructions for selecting the ~~second~~ test in the second wave of tests from a plurality of tests based at least partially upon the network security vulnerability information.

36. (Canceled)

37. (Canceled)

38. (Canceled)

39. (Canceled)

40. (Canceled)

41. (Canceled)

42. (Canceled)

43. (Canceled)

44. (Canceled)

45. (Canceled)

46. (Canceled)

47. (Canceled)

48. (Canceled)

49. (Canceled)

50. (Canceled)

51. (Canceled)

52. (Canceled)

53. (Canceled)

54. (Canceled)

55. (Canceled)

56. (Canceled)

57. (Canceled)

58. (Currently Amended) A network security testing apparatus comprising:

a plurality of testers for generating a security vulnerability attack simulation comprised of a plurality of waves of tests for iteratively testing for network security vulnerabilities of a network system under test to obtain network security vulnerability information;

wherein each of said plurality of testers is adapted to communicably couple to [[a]] the network system under test;

wherein a test of the network system under test is performed by a selected tester of said plurality of testers, said selection of said selected tester to adapt in real rime to ~~detected~~ discovered security obstacles of the network system under test based on the network security vulnerability information gained from a previous test to obtain more specific network security vulnerability information from the network system under test;

wherein said plurality of testers has a load balance characteristic describing a degree of balance of loads of testers of said plurality of testers; and

wherein the selected tester is selected from said plurality of testers based additionally on optimizing the load balance characteristic.

59. (Canceled)

60. (Canceled)

61. (Canceled)

62. (Original) The network security testing apparatus of claim 58,

wherein each tester of said plurality of testers has at least one quality of communicable coupling to the system under test; and

wherein the selected tester is selected from said plurality of testers based at least partially on the selected tester's quality of communicable coupling.

63. (Original) The network security testing apparatus of claim 62, wherein the quality of communicable coupling includes:

cost per bit;

absolute speed; and

geographical proximity of the selected tester to the system under test.

64. (Currently Amended) A network security testing method comprising:

selecting ~~a selected~~ at least one tester from a plurality of testers for generating a security vulnerability attack simulation comprised of a plurality of waves of tests for iteratively testing for network security vulnerabilities of a network system under test to obtain network security vulnerability information, said selection of said ~~selected~~ at least one tester to adapt in real time is modified to discovered security obstacles of the network system under test detected based on network security vulnerability information gained from a previous test to obtain more specific network security vulnerability information from network system under test;

executing a test by the selected tester, wherein the test is targeted at a the network system under test, and wherein the selected tester is communicably coupled to the network system under test;

wherein the plurality of testers has a load balance characteristic describing a degree of balance of loads of testers of the plurality of testers; and

wherein said selecting a selected tester from a plurality of testers is further based at least partially on optimizing the load balance characteristic.

65. (Canceled)

66. (Canceled)

67. (Canceled)

68. (Previously Presented) The network security testing method of claim 64,

wherein each tester of the plurality of testers has at least one quality of communicable coupling to the network system under test; and wherein said selecting a selected tester from a plurality of testers is further based at least partially on the selected tester's quality of communicable coupling.

69. (Previously Presented) The network security testing method of claim 68, wherein the quality of communicable coupling includes:

cost per bit;

absolute speed; and

geographical proximity of the selected tester to the system under test.

70. (Currently Amended) A computer program product for network security testing stored in a computer-readable medium, comprising:

instructions for ~~selecting a~~ at least one selected tester from a plurality of testers for generating a security vulnerability attack simulation comprised of a plurality of waves of tests for iteratively testing for network security vulnerabilities of a network system under test to obtain network security vulnerability information, said selection of said ~~selected~~ at least one tester to adapt in real time is modified to discovered security obstacles of the network system under test detected based on network security vulnerability information gained from a previous test to obtain more specific network security vulnerability information from network system under test;

instructions for executing a test by the selected tester, wherein the test is targeted at a system tinder test, and wherein the selected tester is communicably coupled to the network system under test;

wherein the plurality of testers has a load balance characteristic describing a degree of balance of loads of testers of the plurality of testers; and

wherein the selecting a selected tester from a plurality of testers is further based at least partially on optimizing the load balance characteristic.

71. (Canceled)

72. (Canceled)

73. (Canceled)

74. (Previously Presented) The computer program product of claim 70,

wherein each tester of the plurality of testers has at least one quality of communicable coupling to the system under test; and

wherein the selecting a selected tester from a plurality of testers is further based at least partially on the selected tester's quality of communicable coupling.

75. (Previously Presented) The computer program product of claim 74, wherein the quality of communicable coupling includes:

cost per bit;

absolute speed; and

geographical proximity of the selected tester to the system under test.

76. (Currently Amended) A network security testing apparatus comprising:

[[a]] at least one first tester that is adapted to communicably couple to a network system under test to generate a security vulnerability attack simulation comprised of a plurality of waves of tests to perform network security vulnerability testing, wherein said at least one first tester is adapted to iteratively perform a plurality of waves of tests [[test]] on the network system under test to obtain network security vulnerability information on the network system under test;

wherein each test in the plurality of waves of tests are specifically modified in real-time to adapt to discovered security obstacles of the network system under test detected based on the network security vulnerability information gained from the previous test and to obtain additional network security vulnerability information from the network system under test;

wherein said at least one first tester is adapted to make a first attempt to communicably couple to the network system under test before executing the test to obtain network security vulnerability information;

wherein said at least one first tester is adapted to make a second attempt to communicably couple to the system under test after executing the test to obtain network security vulnerability information ; and

wherein the combination of success of the first attempt and failure of the second attempt are interpreted as detection of the test by the network system under test.

wherein the combination of success of the first attempt and failure of the second attempt are interpreted as detection of the test by the network system under test.

77. (Canceled)

78. (Canceled)

79. (Canceled)

80. (Canceled)

81. (Canceled)

82. (Canceled)

83. (Canceled)

84. (Canceled)

85. (Canceled)

86. (Canceled)

87. (Canceled)

88. (Canceled)

89. (Canceled)

90. (Canceled)

91. (Canceled)

92. (Canceled)

93. (Canceled)

94. (Canceled)

95. (Canceled)

96. (Canceled)

97. (Canceled)

98. (Canceled)

99. (Canceled)

100. (Canceled)

101. (Canceled)

102. (Canceled)

103. (Canceled)

104. (Canceled)

105. (Canceled)

106. (Canceled)

107. (Canceled)

108. (Canceled)

109. (Canceled)

110. (Canceled)

111. (Canceled)